(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
10. Mai 2001 (10.05.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/33801 A2

(51) Internationale Patentklassifikation[7]: H04L 29/06

(21) Internationales Aktenzeichen: PCT/EP00/10568

(22) Internationales Anmeldedatum:
26. Oktober 2000 (26.10.2000)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
199 52 527.7 30. Oktober 1999 (30.10.1999) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: iBRIXX AG [DE/DE]; Schönfeldstrasse 8, 76131 Karlsruhe (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: SCHUSTER, Wolfgang [DE/DE]; Hagsfelder Allee 18, 76131 Karlsruhe (DE).

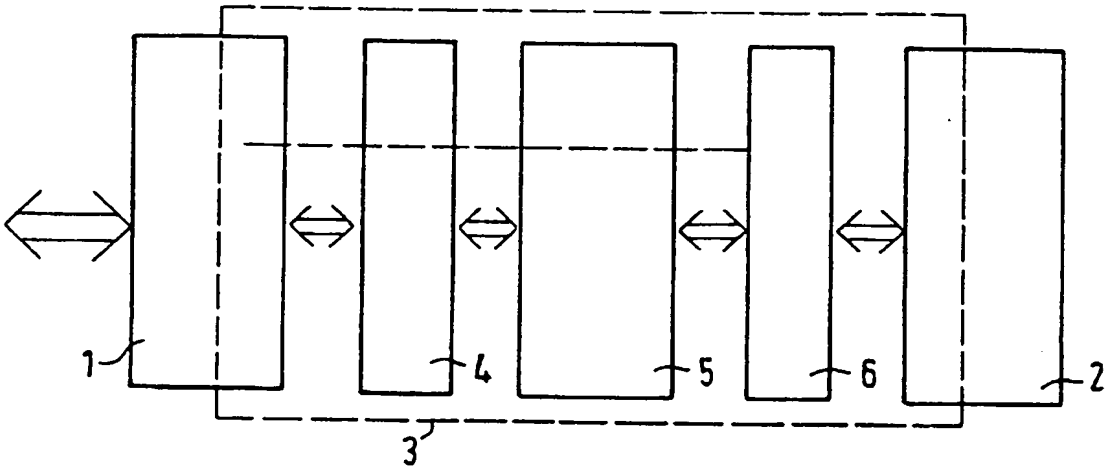
(74) Anwalt: GEITZ & GEITZ; Kriegsstrasse 234, 76135 Karlsruhe (DE).

(81) Bestimmungsstaaten *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK,

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD AND TRANSACTION INTERFACE FOR SECURE DATA EXCHANGE BETWEEN DISTINGUISHABLE NETWORKS

(54) Bezeichnung: VERFAHREN UND TRANSAKTIONSINTERFACE ZUM GESICHERTEN DATENAUSTAUSCH ZWISCHEN UNTERSCHEIDBAREN NETZEN



(57) Abstract: The invention relates to a method and device for ensuring secure data exchange between an internal and an external network, said networks being fully decoupled from each other. This is achieved by means of a transaction interface (3) which creates a waiting list in a neutral area (5) for interrogations which are to be processed. Said interrogations are processed exclusively upon the initiative of and in the region of the secure internal network (2). The waiting list area is secured both externally and internally by corresponding codes and/or an external fire wall (4,6).

(57) Zusammenfassung: Verfahren und Transaktionsinterface zum gesicherten Datenaustausch zwischen zwei unterscheidbaren Netzen. Die Erfindung betrifft ein Verfahren und eine Vorrichtung um den Datenaustausch zwischen einem inneren und einem äußeren Netz bei vollständiger Entkopplung der Netze sicher zu stellen. Diese Aufgabe wird durch ein Transaktionsinterface (3) gelöst, das innerhalb einer neutralen Zone (5) eine Warteschlange der zu bearbeitenden Abfragen einrichtet, wobei die Bearbeitung dieser Anfragen ausschließlich auf Initiative und im

[Fortsetzung auf der nächsten Seite]

WO 01/33801 A2

EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) **Bestimmungsstaaten** *(regional)*: ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

--- *Ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts.*

Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Bereich des gesicherten internen Netzes (2) erfolgt, wobei der Bereich des Warteschlange sowohl nach außen als auch nach innen durch entsprechende Verschlüsselungen und optional durch eine innere und/oder eine äußere Firewall (4, 6) gesichert ist.

VERFAHREN UND TRANSAKTIONSINTERFACE ZUM GESICHERTEN DATENAUSTAUSCH ZWISCHEN UNTERSCHEIDBAREN NETZEN

Die Erfindung betrifft ein Verfahren und Transaktionsinterface zum gesicherten Austausch zwischen unterscheidbaren Netzen, insbesondere zwischen einem externen und einem internen Netz, wie beispielsweise dem Internet und einem firmeneigenen Intranet.

Derartige Verfahren und Vorrichtungen zum gesicherten Austausch zwischen Netzen mit vorzugsweise unterschiedlichen Sicherheitsstandards gehören zum Stand der Technik.

So gehört es zum Stand der Technik, ein internes Datennetz vom externen Netz durch eine sogenannte gesicherte Schnittstelle zu trennen. Die gesicherte Schnittstelle umfaßt dabei im besten Falle einen externen und einen internen Server, die über eine Firewall miteinander in Datenverbindung stehen. Etwaig vom externen Server aufgenommene Kundenanfragen werden im externen Server verarbeitet und nach unterschiedlichen Sicherheitschecks über die Firewall an den internen Server gegeben, der schließlich auf die innerhalb des zu schützenden internen Netzes abgelegten Daten zugreift.

Die zwischen dem internen und externen Server befindliche Firewall soll dabei verhindern, daß von außen, insbesondere mißbräuchliche Transaktionen oder Veränderungen am geschützten Datenbestand des inneren Netzes möglich sind.

Die Firewall verhindert im Ergebnis, daß externe Kunden ohne entsprechende Berechtigung in eine Datenverbindung mit dem internen Netz treten und daß bei bestehender Datenverbindung unzulässige Daten, beispielsweise Virenprogramme durch die Firewall in das interne Netz eingespeist werden. Hierdurch werden zum Beispiel bei fehlender Berechtigung auch an sich zulässige wünschenswerte Kundendienstabfragen die interne Datentransaktionen erfordern, abgeblockt.

Eine übliche Lösung hierfür, besteht in der Öffnung eines zusätzlichen speziellen Kunden-Gateways, der einen entsprechenden Zugriff erlaubt. Dies hat wiederum den Nachteil, daß über dieses zwar besonders gesicherte Gateway nun doch Angriffe auf den internen Datenbestand möglich sind.

Eine andere Lösung beläßt alle etwaigen Kundenfragen auf dem externen Server und vermeidet somit etwaig unerwünschte gefährliche direkte Datenverbindungen nach außen. Nachteilig bei dieser Lösung ist aber, daß etwaig vertrauliche Kundendaten auf einem ungeschützten externen Server zwischengespeichert werden. Aus diesem Grund werden die Daten durch Spiegelung häufig abgeglichen. Dies wird infolge der dadurch wachsenden Datenmenge mit einer erhöhten Prozessorleistung bzw. einem schlechteren Zeitverhalten bezahlt. Außerdem ist bei dieser Lösung ein Zugriff in Echtzeit auf den geschützten Datenbestand des internen Netzes kaum möglich.

Aus der internationalen Anmeldung WO 97/19611 ist zur Lösung dieser Probleme ein sogenanntes „Securite-Gateway-Interface" (SGI) bekannt, das die beschriebenen Probleme dadurch zu lösen versucht, daß aufgrund einer Kundenanfrage zunächst eine Authentikation des Kunden erfolgt und im Falle einer entsprechende Berechtigung des Kunden generiert der externe Server dann anhand der Kundenabfrage eine eigene zulässige Abfrage. Hierdurch ist eine echte Entkopplung zwischen den vom Kunden übermittelten Daten und schließlich zur Weiterbearbeitung vorgesehenen Daten gegeben. Die vom externen Server generierte Anfrage wird schließlich über die Firewall an einen internen Server in unter Abwicklung weiterer Sicherheitsroutinen weitergeleitet und schließlich im internen Netz bearbeitet und über den externen Server eine Antwort an den Nutzer übermittelt. Dieses System stellt somit eine vollständige Entkopplung von internen und externen Netzen sicher. Ungelöst bleibt allerdings das Problem, daß weiterhin vertrauliche Nutzerdaten weitgehend ungeschützt gegen einen Zugriff von außen auf dem externen Server liegen. Falls ein darauf mißbräuchlicher Zugriff auf den äußeren ungeschützten Server gelingt, können hier etwaig nicht zulässige Abfragen durch entsprechend geschickte Manipulation erzeugt werden. Dies ist insbesondere deshalb möglich, weil zwangsläufig die Authentikation der Nutzerabfrage auf dem externen Server erfolgt und somit in dem weitestgehend ungesicherten Bereich des Systems.

Der Erfindung liegt daher die Aufgabe zugrunde, ein Verfahren und eine Vorrichtung zum gesicherten Datenaustausch zwischen unterscheidbaren Netzen zu schaffen, daß eine vollständige Entkopplung der beiden Netze sicherstellt und überdies die erwähnten Nachteile des vorbekannten Standes der Technik vermeidet.

Diese Aufgabe wird durch ein Verfahren zum gesicherten Datenaustausch gemäß Anspruch 1 und ein Transaktionsinterface gemäß Anspruch 15 gelöst.

Dadurch, daß im Unterschied zum Stand der Technik, sämtliche Abfragen externer Nutzer von einem Schnittstellenserver aufbereitet und in definierter Form in einem Schnittstellenspeicher zwischengespeichert werden, die vollständige Bearbeitung dieser Abfragen einschließlich der Authentikation des Nutzers aber innerhalb des gesicherten internen Netzes erfolgt ist keinerlei Zugriff von außen auf sicherheitsrelevante Datenbereiche des internen Netzes möglich.

Vorteilhafte Weiterbildungen der Erfindung ergeben sich aus den Unteransprüchen 2 bis 14.

Gemäß Anspruch 2 wird die im Schnittstellenspeicher angelegte Warteschlange ausschließlich vom inneren Server in einer definierten Frequenz abgefragt. Es ist demnach nicht möglich, aktiv von einem externen Netz aus irgendeine Datentransaktion im inneren Netz auszulösen, da sämtliche Aktionen vom gesicherten Bereich des inneren Netzes ausgehen und auch von hier initiiert werden und schließlich vollständig hier abgewickelt werden. Hierzu zählt insbesondere auch die Authentikation des Nutzers.

Das Sicherheitslevel des Verfahrens kann durch Verwendung einer äußeren Firewall zwischen der neutralen Zone und dem vorgeschalteten externen Netz weiter gesteigert werden. Außerdem ist hierdurch der mißbräuchliche Zugriff auf in der neutralen Zone abgelegte Daten erschwert, auch wenn diese Daten an sich nicht sicherheitsrelevant sind.

In diesem Sinn wird eine weitere Steigerung des Sicherheitstandards durch Zwischenschaltung einer weiteren inneren Firewall zwischen der neutralen Zone und dem internen Netz erreicht. Die innere Firewall stellt auch einen wirksamen Schutz gegen die Spionage von innen, also den Zugriff vom internen Netz auf in der neutralen Zone abgelegten Nutzerdaten sicher.

Die innere Firewall erzwingt eine ausschließlich unindirektionale Kommunikation. Dabei werden Aufrufe grundsätzlich nur aus dem Bereich des internen Netzes akzeptiert. Ein Aufruf aus der neutralen Zone in den Bereich des gesicherten internen Netzes ist nicht möglich.

Die Nutzerabfragen können in unterschiedlichen Datenformaten eingehen. Hierzu kann es sinnvoll sein, in der neutralen Zone einen speziellen externen Server vorzusehen, der für bestimmte ausgewählte Datenformate zuständig ist und die hier eingehenden Nutzerabfragen vor der Weiterleitung an den eigentlichen Schnittstellenserver zunächst konvertiert und ggf. eine Eingangsbestätigung an den Nutzer übermittelt.

Dadurch, daß einmal in der Warteschlange des Schnittstellenspeichers aufgenommene Abfragen bis zu ihrer vollständigen Abarbeitung resistent zwischengespeichert werden, kann die Bearbeitung selbst nach einem vollständigen Systemabsturz im wesentlichen ohne Datenverlust wieder aufgenommen werden. Schlimmstenfalls muß die Bearbeitung der Abfrage wiederholt werden. Hierdurch ist das erfindungsgemäße Verfahren in höchstem Maße störsicher. Dies stellt sowohl eine Maßnahme der Datensicherheit als auch der Bedienerfreundlichkeit dar.

Ein weiteres Leistungsmerkmal des erfindungsgemäßen Verfahrens besteht darin, daß die Bearbeitungsgeschwindigkeit an die jeweilige Last angepaßt werden kann. Dies geschieht gemäß Anspruch 7 zum einen durch lastabhängige Frequenzsteuerung der Abfragen des Schnittstellenspeichers.

Dies kann aber auch mit Vorteil durch das Aktivieren von parallelen Prozessen innerhalb des Schnittstellenservers und/oder des inneren Servers erfolgen. Die Laststeuerung wird dabei mit von dem externen Server des Systems oder mittels eines Laststeuerungsmoduls der Firewall durchgeführt. Dies macht insoweit Sinn, weil die Laststeuerung hierdurch an Stellen angeordnet ist, die in Zugriffsrichtung vor dem Schnittstellenserver und/oder innerem Server liegen und somit die erforderlichen Prozessorkapazitäten bereitstellen können bevor sie benötigt werden. Hierdurch wird ebenfalls die Bedienfreundlichkeit des Systems erhöht.

Neben der softwaremäßigen Zuschaltung und Aktivierung weiterer Prozesse können auch zusätzliche Prozessoraktivitäten gemäß Anspruch 10 durch eine entsprechende Laststeuerung freigegeben oder gesperrt werden.

Die im Schnittstellenspeicher abgelegten Nutzerabfragen werden mit Vorteil verschlüsselt. Die Verschlüsselung dieser Abfragen erschwert den Zugriff von außen aber auch von innen auf etwaig vertrauliche Nutzerabfragen. Hierdurch wird ebenfalls sowohl der Spionage von außen als auch von innen vorgebeugt.

Ein vorteilhaftes Verschlüsselungsverfahren ist gemäß Anspruch 12 gegeben. Hierbei ist ein besonderes Sicherheitsmerkmal durch die individuell vorbestimmbare Lebensdauer der jeweils eingesetzten Schlüssel gegeben. Dies bedeutet, daß selbst falls es einem mißbräuchlich Zugreifenden gelin-

gen sollte, einen eingesetzten Schlüssel zu entschlüsseln, so ist hierdurch längst nicht sichergestellt, daß er einen erfolgreichen Mißbrauch oder gar eine Datentransaktion durchführen kann, da der mit der Schlüsselvergabe definierte Zeitkorridor so eng bemessen ist, daß eine mißbräuchliche Zweitverwendung des Schlüssels schon aufgrund seiner begrenzten Lebensdauer so gut wie ausgeschlossen erscheint.

Ein weiteres wesentliches Sicherheitssmerkmal des Verfahrens liegt darin, daß die Authentikation des jeweiligen Nutzers von der eigentlichen Bearbeitung getrennt erfolgt.

Entscheidend ist gemäß Anspruch 14, daß obwohl die Authentikation des Nutzers vollständig im gesicherten Bereich des internen Netzes vorgenommen wird, zu keinem Zeitpunkt das einem Nutzer jeweils zugeordnete Passwort von der neutralen Zone in das interne Netz oder in umgekehrter Richtung übermittelt wird.

Das Verfahren wird vorteilhaft mit einem Transaktionsinterface gemäß dem unabhängigen Anspruch 15 durchgeführt.

Vorteilhafte Weiterbildungen der erfindungsgemäßen Vorrichtung ergeben sich aus den Unteransprüchen 16 bis 29.

Das Sicherheitsniveau der erfindungsgemäßen Vorrichtung kann gemäß Anspruch 16 oder 17 durch Verwendung einer inneren und/oder äußeren Firewall weiter erhöht werden.

Die Bedienfreundlichkeit und Anwendungsbreite des Transaktionsinterfaces kann durch einen zusätzlichen externen Server, der in der neutralen Zone angeordnet ist, erhöht sein.

Eine dynamische Konfiguration des Transaktionsinterfaces durch ständiges, vorzugsweise periodisches, und vor allem

selbsttätiges Überschreiben der Konfiguration aus dem gesicherten Bereich des internen Netzes stellt ein weiteres Sicherheitsmerkmal dar, da etwaig mißbräuchliche Manipulationen der Konfiguration durch einen unbefugten zugriff aus dem externen Netz, so allenfalls von kurzer Dauer sind und somit insbesondere die Gefahr einer "schleichenden" Infiltration ausgeräumt ist. Es hat sich erwiesen, daß sich langsam aufschaukelnde Eingriffe ein erheblich größeres Risiko darstellen als sofortige und massive Eingriffe, die ebenso schnell bemerkt und bekämpft werden können.

Aus dem gleicher Sicherheitsgedanken heraus ist auch das Überschreiben der statischen Dateninhalte der neutralen Zone in vorgebbaren Zeitabstaänden eine sinnvolle Weiterbildung der Erfindung.

Bei dem erfindungsgemäßen Transaktionsinterface kann zu einer besseren Lastanpassung auch der Schnittstellenspeicher selbst durch eine entsprechende Skalierung an die jeweilige Last angepaßt werden.

Ebenfalls einer besseren Lastansteuerung dient die Anordnung mehrerer Netzwerkrechner innerhalb der neutralen Zone.

Aus dem gleichen Grund können auch mehrerer Netzwerkrechner im Bereich des internen Netzes angeordnet sein.

Dadurch, daß das erfindungsgemäße Transaktionsinterface mit einer CORBA-Schnittstelle versehen ist, können im Bereich des internen Netzes unterschiedliche Betriebssysteme zusammenarbeiten und über das erfindungsgemäße Transaktionsinterface geschützt sein.

In besonders vorteilhafter Ausgestaltung ist das gesamte Transaktionsinterface mit einer durchgehenden CORBA-BUS-Architektur versehen.

Die Kommunikation innerhalb des Transaktionsinterface wird mit Vorteil verschlüsselt abgewickelt, vorzugsweise DES-verschlüsselt.

Dadurch, daß gemäß Anspruch 25 vor der Bearbeitung entsprechender Nutzerabfragen eine Bestätigungsanfrage an den Nutzer übermittelt werden kann, ist das Transaktionsinterface zum korrekten Vertragsabschluß innerhalb des Internets in der Lage. Die hierdurch erlangte nochmalige Bestätigung der Nutzerabfrage oder des Vertrages stellt einen einwandfreien Vertragsschluß im Bereich des e-commerce sicher.

Der gesamte Betrieb des Transaktionsinterfaces wird mittels eines entsprechenden Logging-Moduls innerhalb eines sogenannten Logging-Protokolls aufgezeichnet. In diesem Logging-Protokoll sind sämtliche Transaktionen und Informationen, wie etwa die Verweildauer der jeweiligen Nutzerabfragen in der Warteschlange, die ID der Nutzer u.ä., verzeichnet.

Hierdurch ist es einem Administrator möglich, den Betrieb zu überwachen, etwaige Fehlfunktionen frühzeitig aufzuspüren und insbesondere etwaige Mißbrauchsversuche zu entdekken.

Die Erfindung wird nachstehend anhand eines oder mehrerer in der Zeichnung nur schematisch dargestellte Ausführungsbeispiele näher erläutert. Es zeigen:

Fig. 1 ein Blockschaltbild zum Aufbau des Transaktionsinterfaces,

Fig. 2 ein detailliertes Blockschaltbild des Transaktionsinterfaces,

Fig. 3 ein Laufdiagramm zum Verfahren des gesicherten Datenaustausches und

Fig. 4 ein Blockschaltbild zum Verfahrensablauf,

Fig. 1 zeigt ein externes Netz 1 und ein internes Netz 2, die über ein Transaktionsinterface 3 miteinander in Datenverbindung treten können.

Beim externen Netz 1 handelt es sich zumeist um das Internet, wobei als internes Netz 2 das Intranet eines Unternehmens, häufig ein LAN-Netzwerk, in Frage kommt. Das Transaktionsinterface 3 ist streng genommen nicht abgeschlossen zwischen beiden Netzen angeordnet.

Im Prinzip beginnt der gesicherte Datenaustausch bereits innerhalb des externen Netzes 1 und führt schließlich im Ergebnis zu Transaktionen innerhalb des internen Netzes 2, die anhand der gestrichelten Linie in Fig. 1 verdeutlicht werden soll.

Im übrigen weist das Transaktionsinterface 3 eine äußere Firewall 4 zur Abschottung einer neutralen Zone 5 gegenüber dem externen Netz 2 auf.

Die neutrale Zone 5 ist wiederum gegenüber dem internen Netz 2 durch eine weitere innere Firewall 6 abgeschottet. Die in Fig. 1 symbolisch dargestellten Pfeile symbolisieren nur die Wechselwirkung zwischen den gegeneinander abgegrenzten Bereichen und nicht etwa Datenflußrichtungen.

Wie sich aus der detaillierteren Darstellung in Fig. 2 ergibt, umfaßt die neutrale Zone 5 einen Schnittstellenserver 7 sowie einen externen Server 10. Beim externen Server 10 wird es sich in den allermeisten Fällen um einen üblichen Web-Server handeln. Darüber hinaus ist in der neutralen Zone ein Schnittstellenspeicher 11 vorzugsweise als Bestandteil des Schnittstellenservers 7 vorgesehen. Der Schnittstellenserver 7 steht über die innere Firewall 6 mit einem inneren Server 12, der bereits innerhalb des gesicherten Bereichs des internen Netzes 2 angeordnet ist, in Datenverbindung. Der innere Server 12 ist über eine CORBA-Schnittstelle 13 mit einem oder mehreren Netzservern 14 oder vorzugsweise verteilten Datenbankanwendungen 15 über einen CORBA-BUS 16 verbunden. Der CORBA-BUS 16 stellt ein offenes Bus-System dar, das sich dadurch auszeichnet, daß unterschiedlichste Systeme also auch unterschiedliche Betriebssysteme über diesen CORBA-BUS 16 miteinander kommunizieren können.

So können beispielsweise Unix- oder Windows-Betriebssysteme, Gebäudesteuerungssysteme oder Sun-Workstations über denselben CORBA-BUS 16 angesprochen werden.

Die genannte CORBA-Bus-Architektur wird in bevorzugter Ausführung für den gesamten Datenaustausch innerhalb des Transaktionsinterfaces 3 eingesetzt.

Der genaue Ablauf des Verfahrens zum gesicherten Datenaustausch aufgrund einer Nutzerabfrage, eines sogenannten Requestes, aus dem externen Netz 1 wird nachstehend ausführlich anhand Fig. 3 und 4 erläutert:

Ein externer Nutzer 17 kann sich über das HTP-Protokoll des Internet, beispielsweise ein HTML-Formular zum Datenaustausch mit dem internen Netz 2 beschaffen. Er hat dann Ge-

legenheit, seine Anfrage innerhalb dieses HTML-Formulares zu formulieren. Die Verwendung des HTML-Formulares ist notwendig, weil innerhalb des hier beschriebenen Verfahrens des gesicherten Datenaustausches nur vorbestimmte zulässige Datentransaktionen möglich sind. Insoweit ist durch die Verwendung von HTML-Formularen sichergestellt, daß auch nur diese vorbestimmten Abfragen von den externen Nutzern 17 formuliert werden. Das HTML-Formular wird dann über ein Client-Interface 20, beispielsweise eine Java-Konsole verschlüsselt durch das Internet übertragen und gelangt, sofern der externe Nutzer 17 über die entsprechenden Berechtigungen bzw. Paßworte verfügt, über eine externe Firewall 4 auf den externen Server 10, der innerhalb der neutralen Zone 5 angeordnet ist. Bei dem externen Server 10 handelt es sich im hier vorliegenden Falle um einen Web-Server. Das Transaktionsinterface 3 kann im Rahmen der Erfindung auch mit anderen Datenformaten, wie etwa RMI, in Datenverbindung treten. So kann der Austausch auch mittels älterer Browsertypen oder mit anderen Netzformaten aus dem Internet abgewickelt werden.

Derartige Abfragen werden dann nicht über den externen Server 10 abgewickelt, sondern gelangen direkt auf den Schnittstellenserver 7.

Dabei kann der Webserver 10 durchaus eine eigene Prozessoreinheit oder ein Modul des Schnittstellenservers 7 sein. Es muß sich dabei nicht unbedingt um eine abgeschlossene Rechnereinheit handeln. In dem in Fig. 4 dargestellten Ausführungsbeispiel besteht die neutrale Zone 5 im wesentlichen aus dem Schnittstellenserver 7, der eine ganze Reihe von Modulen aufweist.

Die gestrichelten Pfeillinien innerhalb von Fig. 4 stehen dabei für einen Aufruf, der eine Aktion an der aufgerufenen

Stelle auslöst, und die durchgezogenen Pfeillinien für einen Datenfluß in Pfeilrichtung

Nach Eingang im Webserver 10 wird die aus dem Internet 2 empfangene Abfrage zunächst entschlüsselt ausgelesen und schließlich an den Schnittstellenserver 7 übermittelt. Der Schnittstellenserver 7 weist ein Begrüßungsmodul 21 zur selbsttätigen Bestätigung des Eingangs bzw. zur Begrüßung des Nutzers 17 aus. Vor allem anderen wird eine Eingangsbestätigung bzw. Begrüßung des externen Nutzers 17 über den Web-Server 10 und die äußere Firewall 4 an den Nutzer 17 zurückgegeben.

Je nach Abfrage ist zu diesem Zeitpunkt entschieden und dem Nutzer 17 mitgeteilt worden, ob eine synchrone oder asynchrone Bearbeitung der eingegangenen Abfrage erfolgt. Bei einer synchronen Bearbeitung erhält der externe Nutzer noch in derselben Online-Sitzung das Ergebnis seiner Abfrage.

Im Unterschied hierzu wird bei einer asynchronen Bearbeitung das Ergebnis erst in einer nächsten Online-Sitzung oder in einem gesonderten Vorgang an den externen Nutzer übermittelt. Die Entscheidung, ob eine synchrone oder asynchrone Bearbeitung erfolgt, richtet sich nach Mächtigkeit und Sicherheitsrelevanz der vom externen Nutzer 17 empfangenen Abfrage.

Der Schnittstellenserver 7 beginnt nun die empfangene Anfrage in unkritische Datenpakete zu zerlegen und in eine Warteschlange 22 bzw. 22´einzustellen, die in einem speziellen Schnittstellenspeicher 11 bzw. 11´, der ebenfalls innerhalb der neutralen Zone 5 angeordnet ist.

Dabei wird zumindest in dem hier vorliegenden Ausführungsbeispiel zwischen einer Warteschlange 22 zur Authentikation

des Nutzers 17 und einer Warteschlange 22´ mit der eigentlichen Abfrage unterschieden. In der Regel wird es sich dabei um ein und dieselbe Warteschlange, jedoch unterscheidbare, Speicherbereiche handeln.

Eine herkömmliche Nutzerabfrage umfaßt u.a. auch die Nutzer ID und ein Passwort. Die Nutzer ID wird unter Verwendung des vom Nutzer 17 im Rahmen seiner Abfrage übermittelten Passwortes verschlüsselt in der Warteschlange 22 abgelegt.

Zur Authentikation des Nutzers 17 wird die jeweilige Nutzer ID auf Anfrage des inneren Servers 12 unter Überwindung der inneren Firewall 6, aber ansonsten unverschlüsselt, in den Bereich des internen Netzes 2 an ein Authentifikationsmodul 23 gegeben.

Innerhalb des Authentikationsmoduls 23 wird unter Verwendung des im Bereich des internen Netzes 2 zu der jeweiligen Nutzer-ID abgelegten Passwortes die Nutzer-ID verschlüsselt und über die innere Firewall 6 verschlüsselt in die neutrale Zone 5 zurückgegeben.

In der neutralen Zone 5 wird dann mittels eines in der neutralen Zone implementierten Authentikationsservices 24 des Schnittstellenservers 7 die jeweilige Nutzer-ID unter Verwendung des vom Nutzer 17 eingegebenen Passwortes entschlüsselt und die erhaltene Nutzer-ID mit der zwischengespeicherten Nutzer-ID verglichen.

Für den Fall, daß die beiden ID´s übereinstimmen, wird die Bearbeitung fortgesetzt bzw. freigegeben, ansonsten erfolgt eine entsprechende Miteilung an den externen Nutzer 17.

Bevor die vom externen Nutzer 17 empfangene Abfrage in der entsprechend aufbereiteten Form in die Warteschlange 22´

eingestellt wird, erfolgt eine Verifizierung der Abfrage. Es werden nur solche Datensätze in die Warteschlange eingestellt, die semantisch korrekt sind. Ansonsten wird die Bearbeitung abgebrochen und eine entsprechende Message über den Web-Server 10 an den externen Nutzer 17 abgegeben.

Darüber hinaus wird in der neutralen Zone 5 eine Bearbeitungsprotokoll 25 der aktuell laufenden Bearbeitungen geführt.

Die im Schnittstellenspeicher 11 angelegte Warteschlange 22´ wird in regelmäßigen Abständen vom inneren Server 12 auf etwaig vorhandene und noch zu bearbeitende Abfragen geprüft.

Dies stellt sicher, daß unter keinen Umständen der Zugriff des externen Nutzers 17 irgendeine Aktivität innerhalb des geschützten internen Netzes 2 auslöst, sondern der Zugriff auf die in die Warteschlange 22´ eingestellten Abfragen erfolgt vielmehr selbsttätig von seiten des internen Servers 12. Dies ist ein wesentlicher Aspekt, um etwaige Manipulationen zu verhindern.

Für den Fall, daß auf die vom inneren Server 12 veranlaßte Abfrage der Warteschlange 22´ innerhalb der Warteschlange 22´ noch abzuarbeitende Nutzerabfragen festgestellt werden, werden diese vom inneren Server 12 angefordert. Vor der Übermittlung der Anfrage an den inneren Server 12 erfolgt jedoch zunächst eine Verschlüsselung der Anfrage. Diese Verschlüsselung erfolgt nach dem Verfahren DES mit einer Schlüssellänge von 56 BIT. Selbstverständlich können auch andere Verschlüsselungsverfahren und Schlüssellängen eingesetzt werden. Die eingesetzten Schlüssel werden in einem Schlüsselmanagement überwacht und permanent verändert.

Die Verschlüsselung erfolgt mittels eines bei der Konfiguration des Systems erstellten Basisschlüssel, der eine asynchrone SSL-Verschlüsselung bewirkt. Im weiteren erfolgt dann unter Verwendung dieses Basisschlüssels eine synchrone DES-Verschlüsselung.

Insbesondere haben die eingesetzten Schlüssel nur eine individuell konfigurierbare Lebensdauer. Dies bedeutet, daß mit der Schlüsselvergabe ein schmaler Zeitkorridor zum gesicherten Datenaustausch eröffnet wird. nach Ablauf der Lebensdauer kann der Schlüssel, selbst wenn es einer unbefugten Person gelänge, ihn zu entschlüsseln, nicht mehr genutzt werden. Eine mißbräuchliche Zweitverwertung von Schlüsseln ist hierdurch nahezu ausgeschlossen.

Diese erneute Verschlüsselung der Abfrage vor der Übermittlung an den inneren Server 12 dient in erster Linie dazu, ein Hacking von innen also ein Abhören vertraulicher Nutzerabfragen im Bereich des geschützten inneren Netzes 2 zu vermeiden.

Hierdurch beugt das beschriebene Verfahren im gesicherten Datenaustausch zusätzlich einer Spionage von innen vor.Die derart verschlüsselte Abfrage wird erneut hinsichtlich der Struktur, Inhalt und den Feldinhalten überprüft.

Für den Fall, daß die nunmehr erzeugte Abfrage sich als nicht zulässig erweist, wird an dieser Stelle die Weiterbearbeitung abgebrochen und eine entsprechende Mitteilung an den externen Nutzer 17 übermittelt.

Für den Fall, daß die Abfrage weiter zulässig ist, also einer vorbestimmten Datenabfrage oder Transaktion entspricht, wird die betreffende Abfrage über die innere Firewall 6 des Transaktionsinterfaces 3 an den inneren Server 12 übermit-

telt. Die Datenbankabfrage kann je nach Sicherheitsrelevanz und Mächtigkeit auf einen oder mehreren Servern 12, 12´oder 12´´ unter Hinzuziehung von einer oder mehreren Datenbankanwendungen 15 abgearbeitet werden. Somit werden alle sicherheitsrelevanten Vorgänge im gesicherten Bereich des internen Netzes 2 abgewickelt.

Hierzu muß zunächst die am inneren Server 12 angelangte Abfrage vor der Weiterbearbeitung entschlüsselt werden.

Nach Bearbeitung der Anfrage erfolgt eine Ergebnisausgabe, die verschlüsselt über die innere Firewall 6 an den Schnittstellenserver 7 zurückgegeben wird. Der Schnittstellenserver 7 führt dann eine sogenannte „Matching-Kontrolle" durch; d.h. es wird überprüft, ob das im Bereich des internen Netzes 2 erzeugte Ergebnis mit der Nutzerabfrage im Einklang steht. Falls dies nicht der Fall ist, wird eine Fehlermeldung an den externen Nutzer 17 übermittelt.

Sollte dies der Fall sein, wird das Ergebnis an den Web-Server 10 übermittelt, in ein geeignetes Format umgesetzt und schließlich über die äußere Firewall 4 an das Internet 1 an den externen Nutzer 17 übertragen. Somit ist eine vollständige Datentransaktion unter Verwendung des erfindungsgemäßen Transaktionsinterfaces 3 beschrieben.

Das Transaktionsinterface 3 ist überdies mit einer dynamischen Laststeuerung versehen, die eine Anpassung des Transaktionsinterfaces 3 an den jeweiligen „Traffic" ermöglicht. Zusätzlich kann, wie aus Fig. 4 deutlich wird, anhand des traffics eine lastabhängige Skalierung des Schnittstellenspeichers 11´ erfolgen. Dies wird in Fig. 4 durch die mögliche Vervielfältigung des mit dem Bezugszeichen 11´ versehenen Bereiches dargestellt.

Dies bedeutet, daß der Schnittstellenserver 7 in Abhängigkeit von der anstehenden Last die eingehenden Anfragen entsprechend geschickt in die Warteschlange 11 bzw. 11´ einreiht und bedarfsweise weitere Prozesse also parallele Warteschlangen 11‘ aktiviert, die parallel abgearbeitet werden können. Hierzu können innerhalb der neutralen Zone 5 auch mehrere Schnittstellenserver 7, 7´ bzw. Serverbereiche vorgesehen sein, die je nach Last aktiviert werden. Die Laststeuerung wird dabei entweder vom Web-Server 10 oder von einem Modul der äußeren Firewall 4 übernommen bzw. einem Laststeuerungsmodul 26 des Schnittstellenservers 7.

Das vorbeschriebene Lastmanagement wird vorteilhafterweise gemäß Fig. 6 durch eine entsprechende Laststeuerung auch im Bereich des internen Netzes 2 unterstützt.

So können in Abhängigkeit von der anfallenden Last mehrere innere Server 12, 12‘ aktiviert oder gesperrt werden und zusätzliche Datenbankanwendungen 15 zur Bearbeitung der eingehenden Nachfrage im Bereich des internen Netzes 2 aktiviert werden.

Hierbei ist es hilfreich, das gesamte Transaktionsinterface 3 mit einer durchgängigen CORBA-BUS-Architektur zu versehen, so daß jeder Abfrage eine oder mehrere Serverprozesse zugeordnet werden können.

Der auf Seiten des internen Netzes 2 agierende innere Server 12 ist hierzu mit einer CORBA-Schnittstelle 13 versehen.

Die im System eingesetzten inneren und äußeren Firewalls 4 und 6 können vollkommen herkömmliche Softwareprodukte sein. Der CORBA-Bus ermöglicht im übrigen auf Seiten des internen

Netzes die Zusammenschaltung verschiedener Betriebssysteme wie Windows, NT oder Unix.

Die oben beschriebene spezielle Architektur des Transaktionsinterfaces 3 gestattet es, die im Zusammenhang mit einem wirksamen Vertragsschluß im Bereich des e-commerce erforderlichen Mindestanforderungen zu erfüllen. So kann eine über den Web-Server 10 an den Schnittstellenserver 7 übermittelte Anfrage zunächst dahingehend überprüft werden, ob es sich um eine Vertragsanfrage handelt. Für den Fall, daß es sich um eine derartige Anfrage handelt, kann ein sogenanntes auf den Schnittstellenserver 7 angelegtes Vertragsmodul vor der Weiterbearbeitung zunächst eine Bestätigungsanfrage an den externen Nutzer richten und erst im Falle, daß über den Web-Server 10 diese Bestätigung eingeht, eine Weiterbearbeitung wie oben beschrieben erfolgen.

Der Schnittstellenserver 7 ist darüber hinaus mit einem Logging-Modul versehen, das sämtliche Transaktionen des Transaktionsinterfaces 3 protokolliert. Hierdurch können sämtliche Prozesse ständig von einem Administrator überwacht und gegebenenfalls Fehlfunktionen oder Mißbrauchversuche sofort aufgedeckt werden.

Der Administrator sitzt ausschließlich im Bereich des internen Netzes 2. Die Konfiguration des Transaktionsinterfaces kann nur von hier erfolgen.

Somit ist ein Verfahren und ein Transaktionsinterface 3 zum gesicherten Datenaustausch zwischen zwei unterscheidbaren Netzen 1, 2 gegeben, das bei vollständiger Entkopplung der Netze 1 und 2 mit einer hohen Performance arbeitet und einen Mißbrauch von außen wie von innen unmöglich erscheinen läßt.

B E Z U G S Z E I C H E N L I S T E

1	externes Netz
2	internes Netz
3	Transaktionsinterface
4	äußere Firewall
5	neutrale Zone
6	innere Firewall
7	Schnittstellenserver
10	externer Server
11	Schnittstellenspeicher
12, 12´, 12´´	innerer Server
13	CORBA-Schnittstelle
14	Netzwerkserver
15	Datenbankanwendung
17	externer Nutzer
20	Client-Interface
21	Begrüßungsmodul
22, 22´	Warteschlange
23	Authentikationsmodul
24	Authentikationsservice
25	Sitzungsprotokoll
26	Laststeuerungsmodul

P A T E N T A N S P R Ü C H E

1. Verfahren zum gesicherten Datenaustausch zwischen einem externen und einem internen Netz (1 und 2) über ein Transaktionsinterface (3) hinweg, bei dem ein externer Nutzer vorbestimmte Datentransaktionen innerhalb des internen Netzes (2) vornehmen kann, wobei das Transaktionsinterface (3)
   - ein Portal im externen Netz (1),
   - eine in Zugriffsrichtung dahinterliegende neutrale Zone (5) mit wenigstens
   - einem Schnittstellenserver (7) und
   - einem Schnittstellenspeicher (11),
   - sowie einen inneren Server (12), der bereits innerhalb des internen Netzes (2) angeordnet ist,

   umfaßt,

   dadurch gekennzeichnet,

   - daß Abfragen externer Nutzer (17), die eine Datentransaktion innerhalb des internen Netzes (2) vom Schnittstellenserver (7) aufbereitet und in definierter Form im Schnittstellenspeicher (11) zwischengespeichert werden und
   - die vollständige Bearbeitung einschließlich einer Nutzerauthentikation innerhalb des internen Netzes (2) erfolgt.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß folgende Schritte durchlaufen werden;

- etwaig über das Portal eingegebene Nutzeranfragen werden vom Schnittstellenserver (7), der innerhalb der neutralen Zone (5) angeordnet ist, ausgelesen und ggf. quittiert,
- wobei diese etwaige Quittierung an den Nutzer übermittelt wird,
- der Schnittstellenserver (7) überprüft die Zulässigkeit der Anfrage anhand eines Vergleichs mit einer Menge vorbestimmter zulässiger Anfragen und deren semantische Korrektheit, wobei im Fehlerfalle die Anfrage abgewiesen und ansonsten wie folgt weiter bearbeitet wird -
- im Falle der Weiterbearbeitung stellt der Schnittstellenserver (7) die Anfrage in eine Warteschlange (22, 22'), die innerhalb des Schnittstellenspeichers (11) angelegt ist,
- diese Warteschlange (22, 22') wird in einer definierten Frequenz vom inneren Server (12) abgefragt,
- wobei auf diese Abfrage hin eine Übermittlung der aufbereiteten Anfrage in das interne Netz (2) erfolgt,
- wobei dann die vollständige Bearbeitung einschließlich der Autentikation des Nutzers (17) im internen Netz (2) erfolgt,
- das Ergebnis an den Schnittstellenserver (7) zurückgegeben wird und
- nach einer Überprüfung, ob Ergebnis und Abfrage in Einklang stehen,
- bejahendenfalls eine Antwort an den Nutzer (17) ausgegeben wird.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die Nutzeranfragen vom externen Netz (1)unter Überwindung einer äußeren Firewall (4) in die neutrale Zone (5) gegeben werden.

4. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß der Datenaustausch zwischen der neutralen Zone (5) und dem internen Netz (2) unter Überwindung einer inneren Firewall (6) abgewickelt wird.

5. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß in der neutralen Zone (5) zusätzlich ein externer Server (10), vorzugsweise ein Web-Server, angeordnet ist, wobei zumindest ein Teil der Nutzeranfragen über diesen externen Server (10) an den Schnittstellenserver (7) übermittelt werden.

6. Verfahren nach Anspruch 5, dadurch gekennzeichnet, daß einmal in der Warteschlange (22, 22') des Schnittstellenspeichers (11) aufgenommene Abfragen bis zur vollständigen Abarbeitung oder bis zu einem definierten Zeitablauf resistent gespeichert werden.

7. Verfahren nach Anspruch 6, dadurch gekennzeichnet, daß die Frequenz der Warteschlangen-Abfragen in Abhängigkeit von der Anzahl und/oder der Mächtigkeit der Nutzerabfragen mittels einer entsprechenden Frequenzsteuerung verändert wird.

8. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß in Abhängigkeit von der Anzahl und/oder der Mächtigkeit der Nutzerabfragen parallele Prozesse innerhalb des Schnittstellenservers (7) und/oder inneren Servers (12) freigegeben oder deaktiviert werden.

9. Verfahren nach Anspruch 8, dadurch gekennzeichnet, daß innerhalb der neutralen Zone (5) mehrere Schnittstellenserver (7) angeordnet sind, die je nach Anzahl und/oder Mächtigkeit der Nutzeranfragen aktiviert oder deaktiviert werden, wobei die hierzu erforderliche Laststeuerung mittels des externen Servers (10) und/oder mittels eines Laststeuerungsmoduls der äußeren Firewall (4) erfolgt.

10. Verfahren nach Anspruch 8 und 9, dadurch gekennzeichnet, daß innerhalb des internen Netzes (2) mehrere innere Server (12) angeordnet sind, die je nach Anzahl und/oder Mächtigkeit der Nutzeranfragen aktiviert oder deaktiviert werden, wobei die hierzu erforderliche Laststeuerung mittels des Schnittstellenservers (7) und/oder mittels eines Laststeuerungsmoduls der inneren Firewall (6) erfolgt.

11. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die Nutzerabfragen vor Ihrer Übermittlung in die innere Zone (2) innerhalb der neutralen Zone (5) verschlüsselt werden.

12. Verfahren nach Anspruch 11, dadurch gekennzeichnet, daß die zur Verschlüsselung jeweils eingesetzten Schlüssel eine individuell vorbestimmbare Lebensdauer haben.

13. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die Authentikation des Nutzers (17) unabhängig von der sonstigen Bearbeitung der Nutzerabfrage erfolgt.

14. Verfahren nach Anspruch 13, dadurch gekennzeichnet. daß die zur Authentikation des Nutzers (17) folgende Schritte durchlaufen werden;

- Separierung einer Nutzer-ID und eines Nutzerpasswortes aus der Nutzerabfrage in der neutralen Zone (5),
- auf Anfrage des inneren Servers (12) Übermittlung der Nutzer-ID an das interne Netz (2),
- Verschlüsselung der Nutzer ID im inneren Netz (2) unter Verwendung des im inneren Netz (2) zu dieser Nutzer-ID abgelegten Passwortes,
- und Rückgabe der solcherart verschlüsselten Nutzer ID in die neutrale Zone (5),
- Entschlüsselung der aus dem inneren Netz(2) zurückgegebenen Nutzer-ID unter Verwendung des vom Nutzer (17) eingegebenen und in der neutralen Zone (5) zwischengespeicherten Passwortes,
- Vergleich der entschlüsselten Nutzer ID und der vom Nutzer eingegebenen, wobei im Falle der Übereinstimmung die Authentizität des Nutzers bestätigt und andernfalls verneint wird und Abhängigkeit hiervon die Nutzerabfrage weiter bearbeitet wird oder nicht.

15. Transaktionsinterface zum gesicherten Datenaustausch zwischen einem externen und einem internen Netz (1 und 2), bei dem ein externer Nutzer (17) vorbestimmte Datentransaktionen innerhalb des internen Netzes (2) auslösen kann und hierzu das Transaktionsinterface (3)

- eine neutrale Zone (5), die in Zugriffsrichtung hinter einem Portal im externen Netz (1) angeordnet ist und wenigstens einen Schnittstellenserver (7), sowie
- wenigstens einen Schnittstellenspeicher (11) aufweist,
- wenigstens einem inneren Server (12), der innerhalb des internen Netz (2) angeordnet ist, umfaßt,

dadurch gekennzeichnet,

- daß innerhalb des Schnittstellenspeichers (11) eine Warteschlange (22, 22') zur Zwischenspeicherung von Nutzeranfragen angelegt ist,
- die in einer definierten Frequenz vom inneren Server (12) abfragbar ist und
- daß nach Übermittlung der entsprechend aufbereiteten Anfragen an den inneren Server (12) die vollständige Bearbeitung der Anfragen, einschließlich der Nutzerauthentikation, innerhalb des internen Netzes (2) vorgesehen ist.

16. Transaktionsinterface nach Anspruch 15, dadurch gekennzeichnet, daß die neutrale Zone (5) gegenüber dem externen Netz (1) mittels einer äußeren Firewall (4) abgeschottet ist.

17. Transaktionsinterface nach Anspruch 15 oder 16, dadurch gekennzeichnet, daß das interne Netz (2) gegenüber der neutralen Zone (5) mittels einer inneren Firewall (6) abgeschottet ist.

18. Transaktionsinterface nach einem der Anspruch 15 bis 17, dadurch gekennzeichnet, daß innerhalb der neutralen Zone (5) zusätzlich ein externer Server (10) vorgesehen ist, der aus dem externen Netz(1) unmittelbar oder mittelbar über den Schnittstellenserver (7) zur Bearbeitung von Nutzerabfragen ansprechbar ist.

19. Transaktionsinterface nach einem der Ansprüche 15 bis 18, dadurch gekennzeichnet, daß die Konfiguration des Transaktionsinterfaces (3) in vorgebbaren Zeitabständen aus dem internen Netz (2) selbsttätig überschrieben wird.

20. Transaktionsinterface nach einem der Ansprüche 15 bis 19, dadurch gekennzeichnet, daß in der neutralen Zone (5) abgelegte Daten in vorggebbaren Zeitabständen aus dem internen Netz (2) selbsttätig überschrieben werden.

21. Transaktionsinterface nach einem der Ansprüche 15 bis 20, dadurch gekennzeichnet, daß der Schnittstellenspeicher (11) derart skalierbar ist, daß aus dem externen Netz (1) eingehende Nutzerabfragen je nach Umfang und Dringlichkeit entsprechend in die Warteschlange (22, 22') des Schnittstellenservers (7) einsortiert und gegebenenfalls zusätzliche Prozesse aktivierbar sind.

22. Transaktionsinterface nach Anspruch 21, dadurch gekennzeichnet, daß innerhalb der neutralen Zone (5) mehrere Netzwerkrechner angeordnet sind, auf denen jeweils ein Schnittstellenserver (7) angeordnet ist, wobei in Abhängigkeit von der Anzahl und/oder Mächtigkeit der Nutzeranfragen zusätzliche Server (7) aktiviert oder deaktiviert werden können, wobei die Laststeuerung vom

externen Server (10) und/oder der äußeren Firewall (4) erfolgt.

23. Transaktionsinterface nach Anspruch 20 oder 2119, dadurch gekennzeichnet, daß im Bereich des internen Netzes (2) mehrere Netzwerkrechner angeordnet sind, die jeweils mit einem inneren Server (12) versehen sind, die je nach Umfang und Mächtigkeit der Nutzeranfragen aktivierbar oder deaktivierbar sind, wobei die Laststeuerung von der inneren Firewall (6) bzw. einem oder mehreren Schnittstellenservern (7) übernommen wird.

24. Transaktionsinterface nach einem der vorhergehenden Ansprüche 15 bis 23, dadurch gekennzeichnet, daß der innere Server (12) über einen CORBA-Bus mit dem internen Netz (2) kommuniziert

25. Transaktionsinterface nach Anspruch 22, dadurch gekennzeichnet, daß das gesamte Transaktionsinterface (3) über ein durchgehendes CORBA-Bus-System in Datenverbindung steht.

26. Verfahren nach einem der vorhergehenden Ansprüche 15 bis 23, dadurch gekennzeichnet, daß die gesamte interne Schnittstellenkommunikation SSL-verschlüsselt, vorzugsweise DES verschlüsselt, erfolgt.

27. Verfahren nach einem der vorhergehenden Ansprüche 15 bis 24, dadurch gekennzeichnet, daß der Schnittstellenserver (7) vor der Einstellung bestimmter Nutzeranfragen eine Bestätigungsanfrage an den Nutzer (17) übermittelt und erst nach Eingang der Bestätigung die Weiterbearbeitung erfolgt.

28. Verfahren nach einem der vorhergehenden Ansprüche 15 bis 25, dadurch gekennzeichnet, daß mittels eines Logging-Moduls ein Logging-Protokoll aufgezeichnet wird, das sämtliche über das Transaktionsinterface (3) abgewickelten Transaktionen aufzeichnet.

29. Verfahren nach einem der vorhergehenden Ansprüche 15 bis 26, dadurch gekennzeichnet, daß die Konfiguration des Schnittstellenservers (7) ausschließlich aus dem internen Netz (2) durchführbar ist.

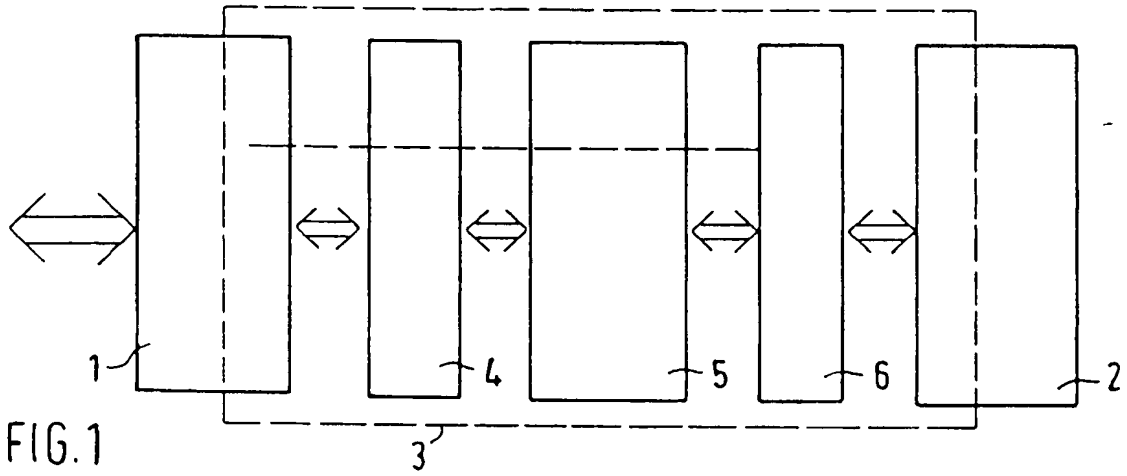


FIG.1

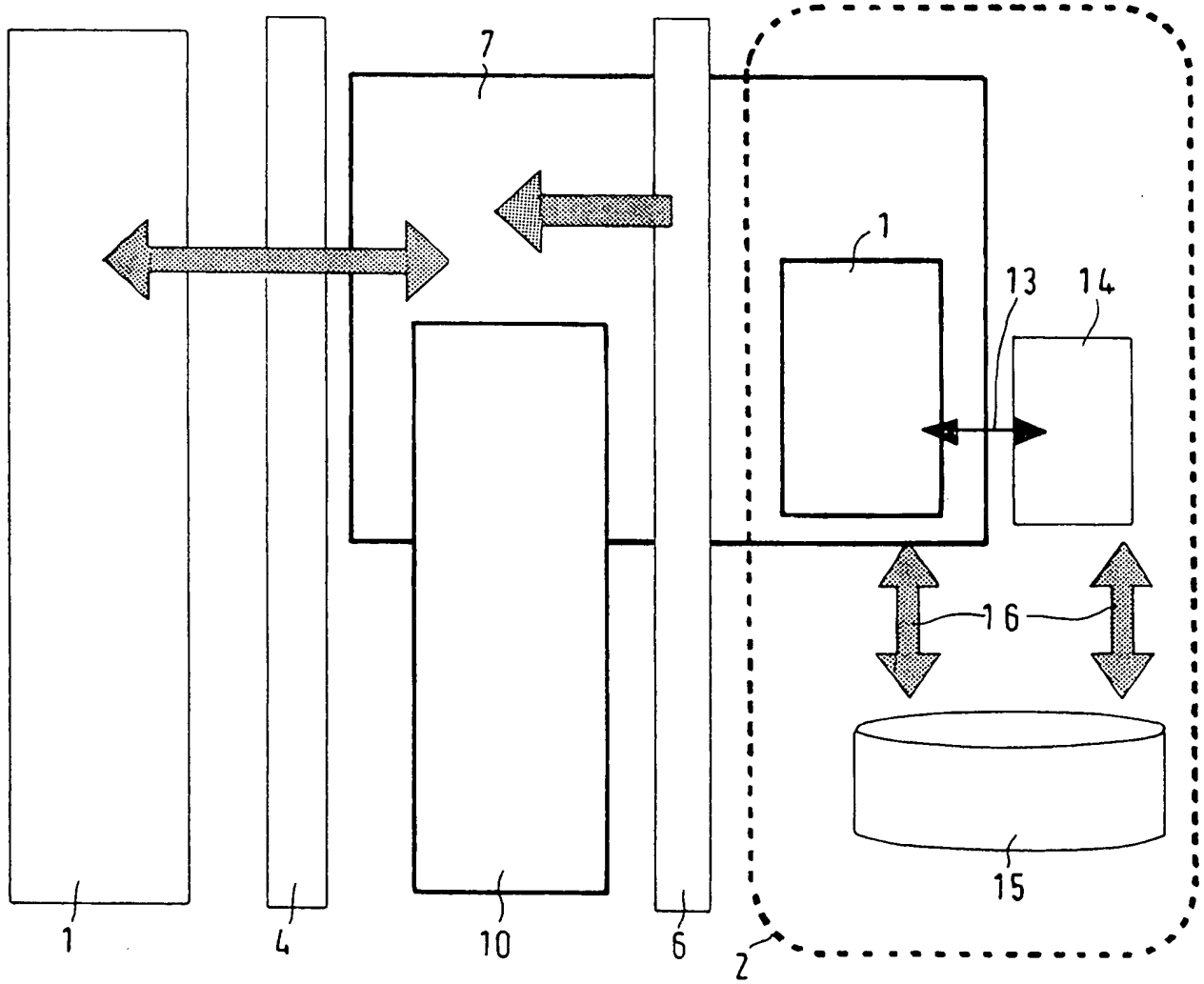


FIG.2

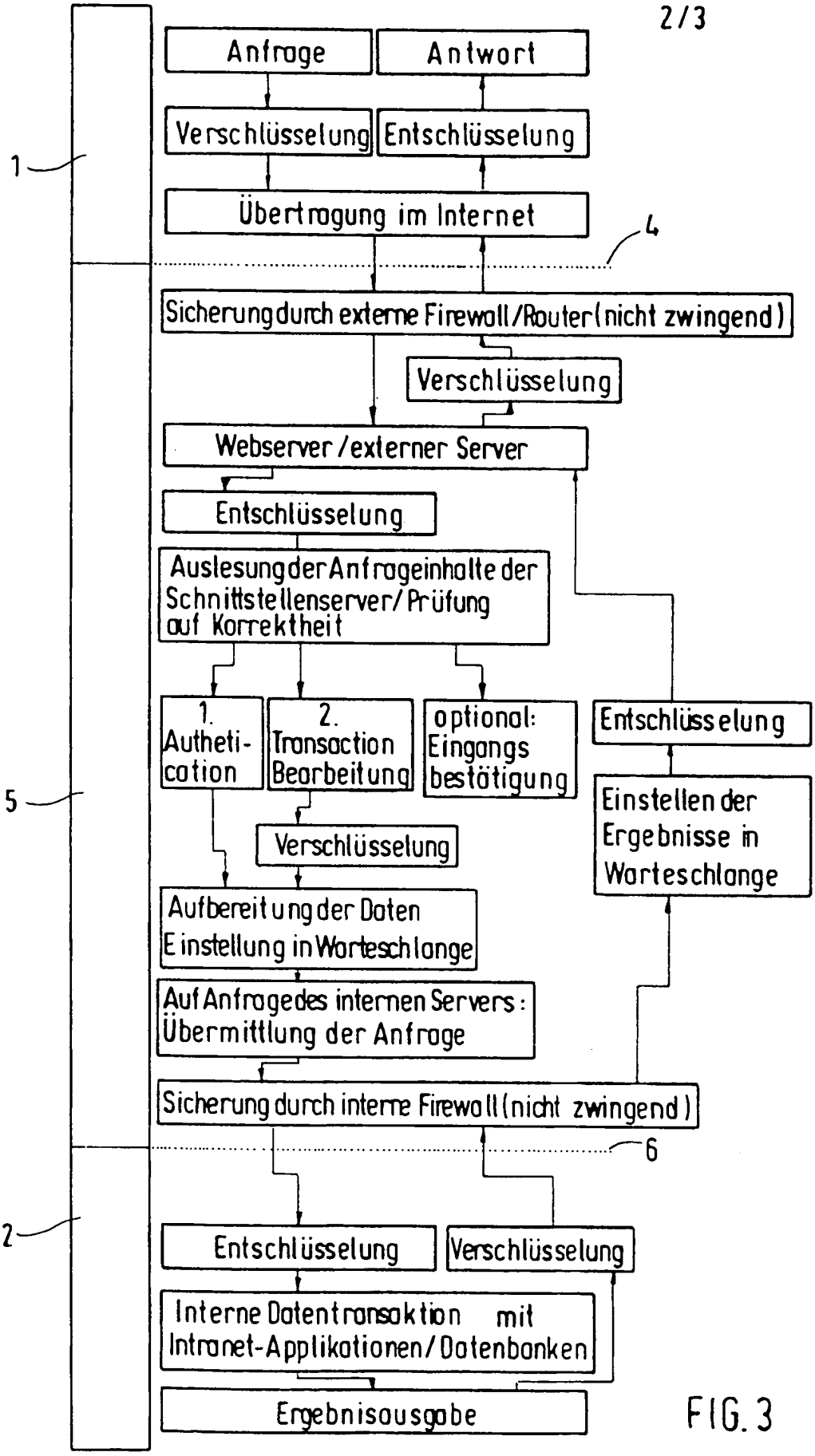

Anfrage
Antwort
Verschlüsselung
Entschlüsselung
Übertragung im Internet
1
4
Sicherung durch externe Firewall/Router (nicht zwingend)
Verschlüsselung
Webserver/externer Server
Entschlüsselung
Auslesung der Anfrageinhalte der Schnittstellenserver/Prüfung auf Korrektheit
1. Authetication
2. Transaction Bearbeitung
optional: Eingangs bestätigung
Entschlüsselung
Einstellen der Ergebnisse in Warteschlange
5
Verschlüsselung
Aufbereitung der Daten Einstellung in Warteschlange
Auf Anfrage des internen Servers: Übermittlung der Anfrage
Sicherung durch interne Firewall (nicht zwingend)
6
2
Entschlüsselung
Verschlüsselung
Interne Datentransaktion mit Intranet-Applikationen/Datenbanken
Ergebnisausgabe

FIG. 3

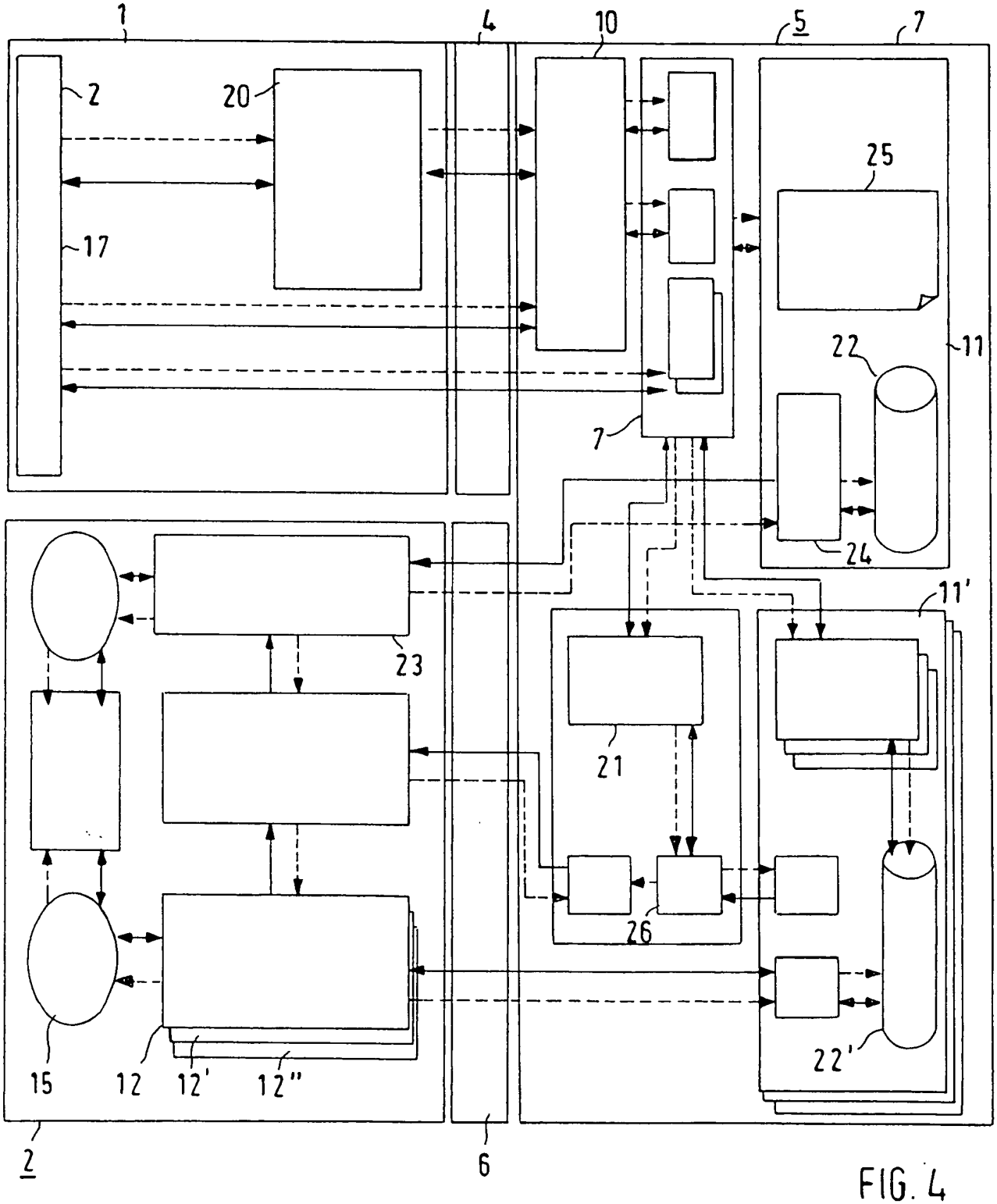


FIG. 4